	FACSIMILE ELECT	TRO MAIL TRANSMITTAL	1/1
(This infor	metion collection is not subject to O	MB review under PL-96, The Paperw	rork Reduction Act.)
		TON OVER UNSECURED TELECO	
OFFICIAL DOD	TELECOMMUNICATIONS SYST	TEMS ARE SUBJECT TO MONIT	ORING AND USE OF DOD   '
		UTES CONSENT TO MONITORIN	<u>6</u> .
SECTION 1 - TO BE COMPLET			+
CLASSIFICATION	TRANSMISSION		
UNCLAS		EDIATE ROUTINE	PAGE 1 OF PAGES
FOR OFFICIAL USE ONLY			
O (Office Symbol, Point of Conta	et and Address)		FAX NO.
(b)(6),(b)(7)(C)		DSN	(b)(6),(b)(7)(C)
BI CITAC			
BICITAC		1	
		-	OICE NO.
		DSN	COMMERCIAL
LECTRONIC MAIL ADDRESS IE-A	Apill		
TO LUCKY MUIC MOULES IN			
IBJECT			•
dministrator/Owner states	(b)(6),(b)(7)(C)		
untiling a story Owner States	Ett nom		
NOM (Office Symbol, Point of Co.	amet and Address		FAX NO
	THE STO PROPERTY.	DSN	COMMERCIAL
A (b)(6),(b)(7)(C)		1 55.1	
Q AFOSI/XOII			(b)(6),(b)(7)(C)
Q AL OSHAOL			
		V	OICE NO.
	·	DSN	COMMERCIAL
ECTRONIC MAIL ADDRESS IE-M	(a)(i)	-	
PERIODIC MUIE ADDICES IE-III		(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)
EMARKS		•	
	200 110	12(120)	
(6),(b)(7)	288-HQ	- 1242560	
(6),(b)(7)	288-HQ	- 1242560	
(6),(b)(7)	288-HQ		
(6),(b)(7)			trying to get through the system
(6),(b)(7)	still reading it. Looks like lots of		trying to get through the system
ere's that statement - I'm			trying to get through the system
ere's that statement - I'm segs right now. Monitor is	still reading it. Looks like lots of		trying to get through the system
ere's that statement - I'm segs right now. Monitor is	still reading it. Looks like lots of		trying to get through the system
lere's that statement - I'm sogs right now. Monitor is	still reading it. Looks like lots of		trying to get through the system
(ere's that statement - I'm sugs right now. Monitor is	still reading it. Looks like lots of		trying to get through the system
(6),(b)(7)  lere's that statement - I'm segs right now. Monitor is to (6),(b)(7)(C)	still reading it. Looks like lots of		trying to get through the system  A 21258  A 21258
lere's that statement - I'm sogs right now. Monitor is	still reading it. Looks like lots of		trying to get through the system  A 21268  D 21268  D 21268
ogs right now. Monitor is 1	still reading it. Looks like lots of	f good info. Our guys are on site lata yet.	trying to get through the system  A 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
(6),(b)(7)(C)  (b)(6),(b)(7)(C)	still reading it. Looks like lots of	f good info. Our guys are on site lata yet.	trying to get through the system  A 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
(6),(b)(7)(C)  (b)(6),(b)(7)(C)	still reading it. Looks like lots of	f good info. Our guys are on site lata yet.  DATE	trying to get through the system    1
(6),(b)(7)  erc's that statement - I'm ags right now. Monitor is to (6),(b)(7)(C)  (b)(6),(b)(7)(C)	still reading it. Looks like lots of up and running there. No new d	f good info. Our guys are on site lata yet.	TIMID / C
ere's that statement - I'm s gs right now. Monitor is (6),(b)(7)(C)  (b)(6),(b)(7)(C)  LEASER'S  CTION II - TO BE COMPLETE	still reading it. Looks like lots of up and running there. No new d	f good info. Our guys are on site lata yet.  DATE  12 Feb 98	TIMID / C
(6),(b)(7)(C)  lerc's that statement - I'm sogs right now. Monitor is (6),(b)(7)(C)  (b)(6),(b)(7)(C)  (c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(c)(	still reading it. Looks like lots of up and running there. No new d	f good info. Our guys are on site lata yet.  DATE	TIMID / C
(6),(b)(7)  Gerc's that statement - I'm sigs right now. Monitor is (6),(b)(7)(C)  (b)(6),(b)(7)(C)  (c)  (c)  (c)  (c)  (d)  (d)  (d)  (e)  (e)  (e)  (e)  (e	still reading it. Looks like lots of up and running there. No new d	f good info. Our guys are on site lata yet.  DATE  12 Feb 98	TIMID / C
(6),(b)(7)(C)  (b)(6),(b)(7)(C)  (b)(6),(b)(7)(C)	still reading it. Looks like lots of up and running there. No new d	f good info. Our guys are on site lata yet.  DATE  12 Feb 98	TIMID / C
(6),(b)(7)  erc's that statement - I'm gs right now. Monitor is to (6),(b)(7)(C)  (b)(6),(b)(7)(C)  LEASER'S  CTION II - TO BE COMPLETE LYE TRANSMITTED	still reading it. Looks like lots of up and running there. No new do not be and running there. No new do not be a new do not b	f good info. Our guys are on site lata yet.  DATE  12 Feb 98  TRANSMITTER'S SIGNATURE	TIMID / C
ere's that statement - I'm set of statement is the statement of the set of statement of sta	still reading it. Looks like lots of up and running there. No new d	f good info. Our guys are on site lata yet.  DATE  12 Feb 98	TIMID / C
(b)(6),(b)(7)(C)  (b)(6),(b)(7)(C)  (b)(6),(b)(7)(C)  EASER'S  THON II - TO BE COMPLETE E TRANSMITTED	still reading it. Looks like lots of up and running there. No new do not be and running there. No new do not be a new do not b	f good info. Our guys are on site lata yet.  DATE  12 Feb 98  TRANSMITTER'S SIGNATURE	TIMID / C

FEB-12-1998 09:30

	P.02/16
USPECT	OMB No. 0701-0128
WITNESS/COMPLAINANT	Expirus Apr 30, 1997

ECT/WITNESS/COMPLAINANT STATEMENT OF SUS aring this burden, to Department of Defense, WHS, DIGR, 1216 Justianan Devis Highway, Suste 1204, Adington VA 22202-4302; and to DMN. rock Production Product 80701-0128), Washington DC 20603, Phases DO NOT RETURN your form to either of treas address PRIVACY ACT STATEMENT AUTHORITY: 10 U.S.C. 8013; 44 U.S.C. 3101; - 60 9397 PRINCIPAL PURPOSES. Used to record information and details of criminal actually which may receive investigative action by comm est; and to provide information to appropriate individuals within DaD expendentials who about proper local and administrative action is taken. ROUTINE USSS: information may be disclosed to local, namely, state and federal law enforce usion arranged from this form may be used in other method criminal and/or club proceeding DISCLOSURE IS VOLUNTARY! SSN Is used to perfectly Distry of individual interior the district." I. STATEMENT INFORMATION UNIT TAKING STATEMENT REPEAT III known! DATE LOCATION AND INSTALLATION (Bidg/Room No) AROSE DET 401 OFFENSE 1749 11FEB 98 COMPLAINT ANDOLPH AFBITX H. PERSONAL IDENTIFICATION (Print or Type) SCN STATUS/GRADE NAME (Last First, Middle Initial) (b)(6),(b)(7)(C) (b)(6)(b)(7)(C GIV TELEPHONE LOCAL ADDRESS (Include Zip Code) DATE AND PLACE OF BIRTH IH required! HOME DUTY PERMANENT ADDRESS OR HOME OF RECORD (Include Zip Code) MILITARY ORGANIZATION/EMPLOYER DEROS NA SPONSOR INFORMATION NAME (Love First Middle Inhla) GRADE DAGANIZATION DUTY PHONE III. ACKNOWLED GEMENT OF OFFENSES AND 5TH AMENDMENT/ARTICLE 31 RIGHTS ADVISEMENT (Suspect Only) there been advised that I om suspected of the following offeness: ADVISED BY IFUN Name and Ranki INDIVIDUAL IDENTIFIED HIMSELF HERSELF AS A ISP. MODIOI OPONE OTO. and advised me that I have the following rights according to the 5th Amendment of the U.S. Constitution/Article 31 of the SUSPECT Uniterm Code of Military Justice NITIALS I have the right to remain alent - that is to say nothing at all. Any statement I make, and or witte s evidence against me in a trial or in other judicial, non-judicial, or administrative proceedings. I have the right to consult with a lawyer. I have the right to have a lewyer present during his interview. I may obtain a civilian lawyer of my own choice at the expense the the government. I may request a lewyer eny time during this interview. If I decide to enswer questions with or without a lawyer present A may stop the questioning at any time. MILITARY ONLY: If I want a military lawyer, one will be appointed for me free of charge. CIVILIANS ONLY: If I conner offerd a lawyer and want one, a lawyer withte appointed for me by civilian authorities. SUSPECT I have read my rights as kited above and I fully understand my rights. No promises, threats, or inducements of any kind have been made to me. Ne pressure or coercion has been used against me. I make the following choice. (Initial One) I do not want a lawyer. I am willing to answer questions or make a statement or both, about the offense(s) under investigation. I do not want a lawyer and I do not wish to make a statement or answer any questions. I want a lawyer. I will not make any statement or enswer any questions until I talk to a lawyer. I fully understand my rights and that my algorithm does not constitute an admission of guit. SIGNATURE OF SUSPECT SIGNATURE OF WITNESS/INTERVIEWER

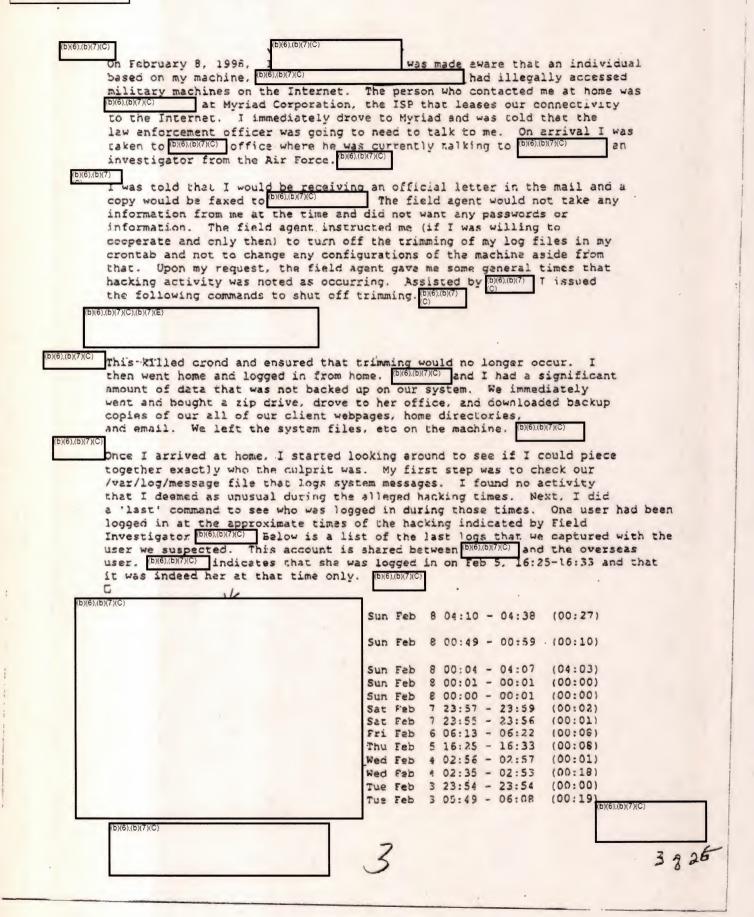
AF FORM 1168, JUL 95 (LRA)

PREVIOUS EDITIONS ARE OSBOLETE.

OF PAGES PAGE 1

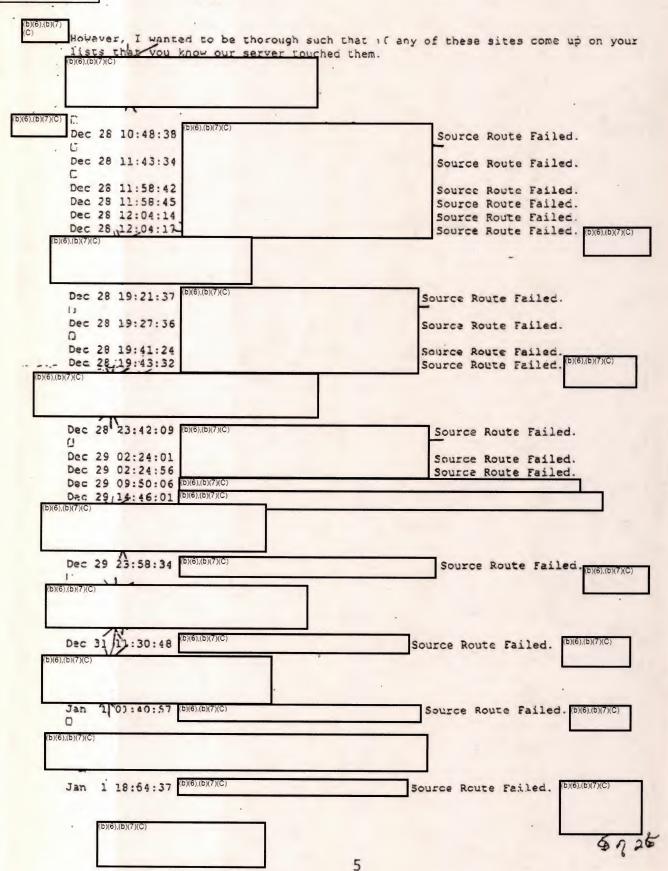
288-46-1340-0-60

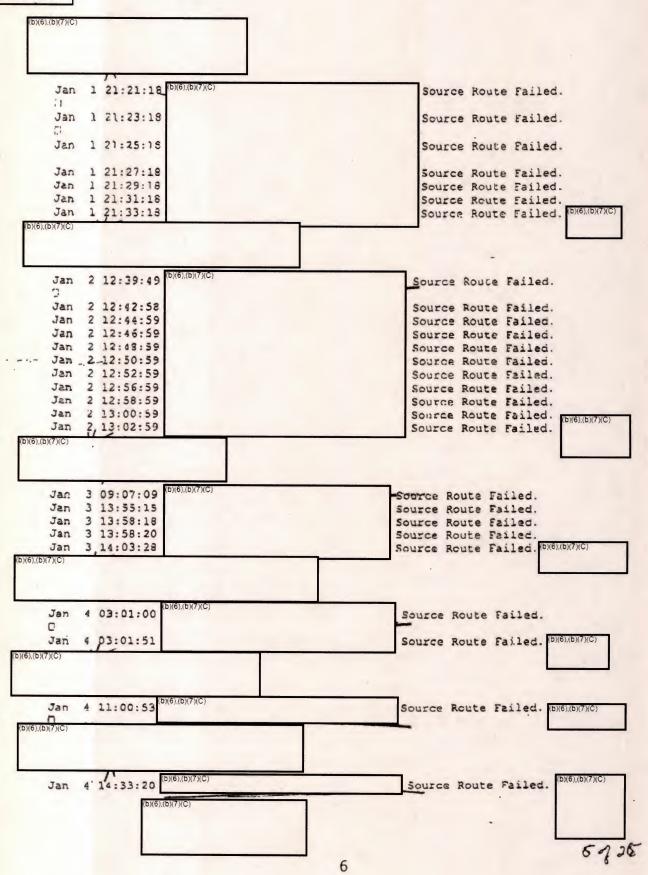
(b)(6)(b)(7)(C)



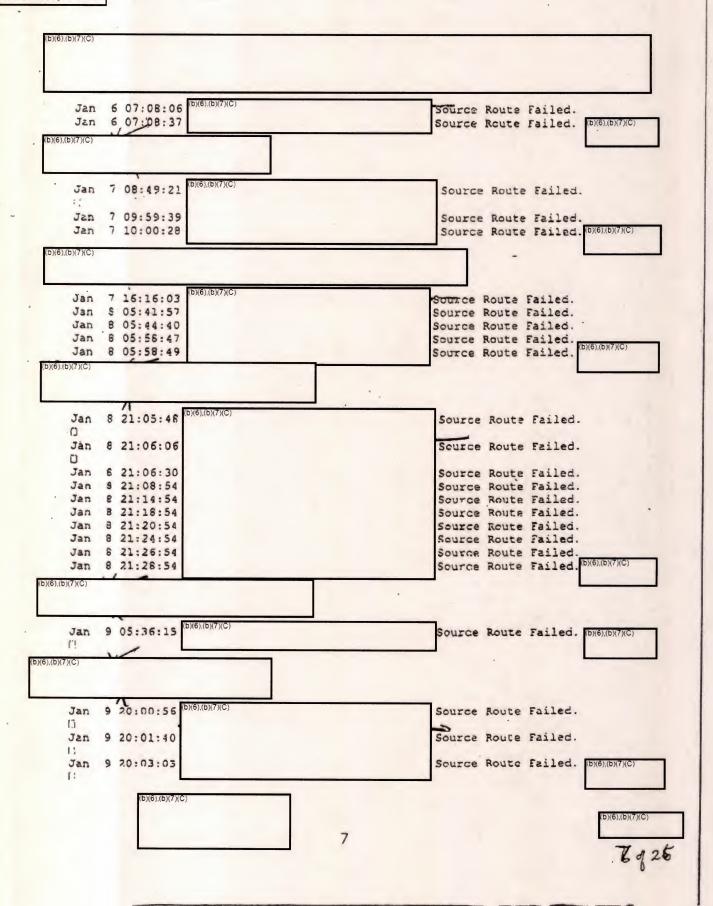
(b)(6),(b)(7)(C)					
			3 05:46 - 05		
			3 05:04 - 05		
			3 04:50 - 04		
		Tue Feb	3 04:32 - 04	:37 (00:05) (b)(6),(b)(	(7)(C)
(b)(6),(b)(7)				VENCEN (BVZVC)	
(C) I have high	nlighted a time range that	it seemed t	o match with	what (b)(b)(b)(r)(c)	
indicated.	However, I now see that	: I jumped	the gun a bit	in that the date	WES
	(b)(7)(C) indicated a break 1				
	ding to this last log, I				
	The wtmp file was set to				
space than	security so more data is	not avail	able. In my	haste I accidenta	lly
	last' that contained all				
	on the tape restored syst	em once th	e court order	is obtained. (D)(6),(D	)(7)(C)
(b)(6),(b)(7) (C)					
would lik	ce to have a note made th		I have seen t	he bat account lo	gged
	sly from two locations: (b)	(6),(b)(7)(C)			
(b)(6),(b)(7)(C)					
-3					
15					
About this	time, I was contacted by	.znother f	ield investig	ator, (D)(D)(/)(C)	
(b)(6),(b)(7)(C)	•				
CACAMEAN ACA	arranged an appoint	ment to me	et me at my s	ervice providers	
	re the machine resides.				
	y drives. It was totall				
perfectly c	lear to me that I didn't	have to b	ackup the hard	d drives or	
cooperate W	with them at all. (b)(6),(b)(7)	also gave :	ma some file	names that	
	had placed on previous s			king for	
information (6),(b)(7)(C)	. The files he named we	re as foll	ows: (b)(6),(b)(7)(C	)	
NO, NO, NO,					
After he ca.	Iled, I started poking a	round on my	y system some	more. I edited	no
files, nor	did I create any files i	n system a:	reas. All tha	et I have include	d
were taken	from telnet session logs	. I examin	ned the ftp lo	ogs and the messa	åe
logs. I for	und nothing that I felt	was importa	ant. Then I s	started looking for	or
files on the	e system that had been re	ecently upo	isted. I four	nd some suspicious	s
	y a file names (b)(6),(b)(7)(C)	in one of t	the /var direc	tories. The con-	tents
The state of the s			to make out t		
contained a	list of all the files in	n my root o	directory tree	(b)(6),(b)(7)(C)	
b)(7)(C)					
After this I	I went to sleep. I awoke	e the follo	owing morning	and started	
working on g	getling information from	my server.	This was 2/	9/98 around 08:00	D. I
	nd checked /var/lcg/mess			errors for many	
	P numbers. (b)(6),(b)(7)(C) logge			account	
and did a lo	pokup on the ip numbers.	Many were	.af.mil site	s. We	
immediately	paged (b)(6),(b)(7) and left a n	nassace for	(D)(6),(D)(7)(C)		
0)(6),(b)(7)					
11615 13 4 61	ranscript from the log fi				
we saw and t	the hosts they belonged t	o wore ins	erted and are	preceded by >.	Ibv6\/bv7\/o\
know that so	ome of these are probably	related t	o the apache	httpd on my syste	m. (D)(0)(D)(7)(C)
(b)(6),(b)(7)(	(C)				(b)(6),(b)(7)(C)
(0)(0),(0)(1)(	(~)				

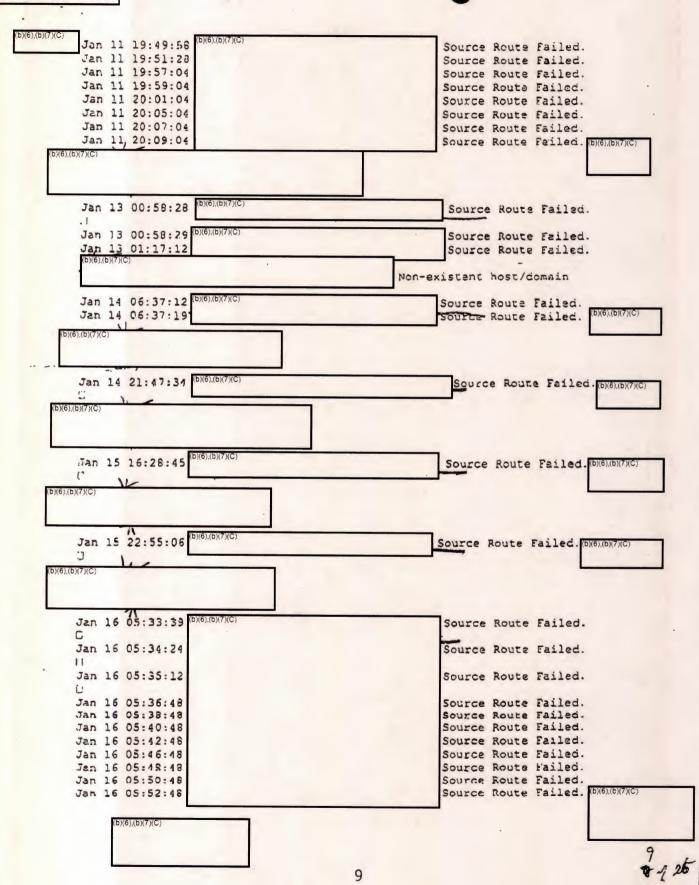
4 1 26

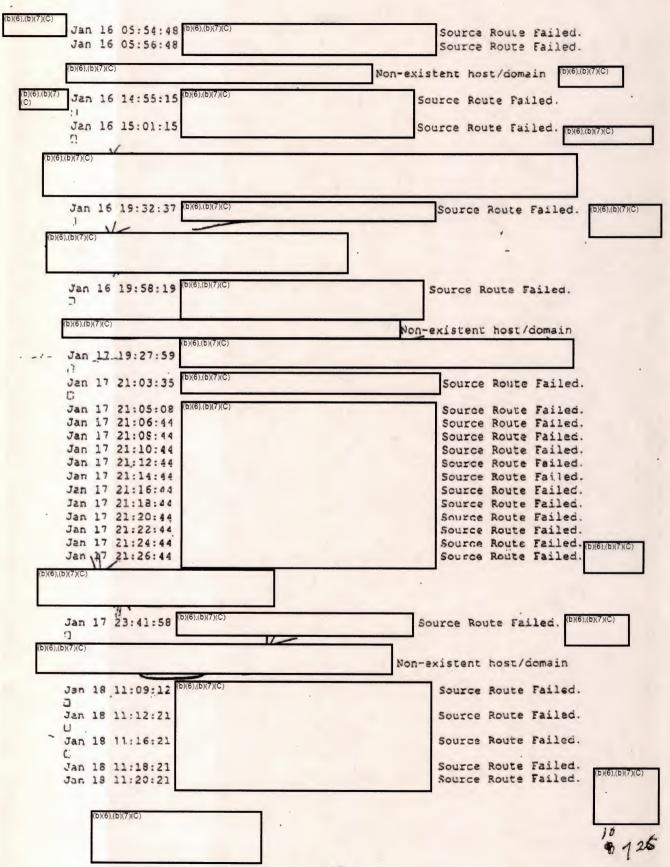


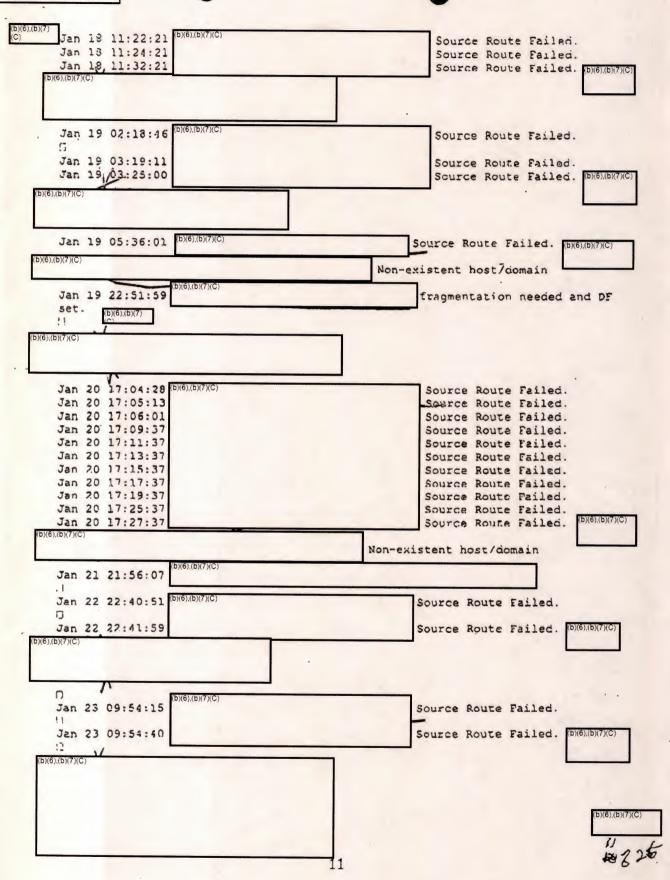


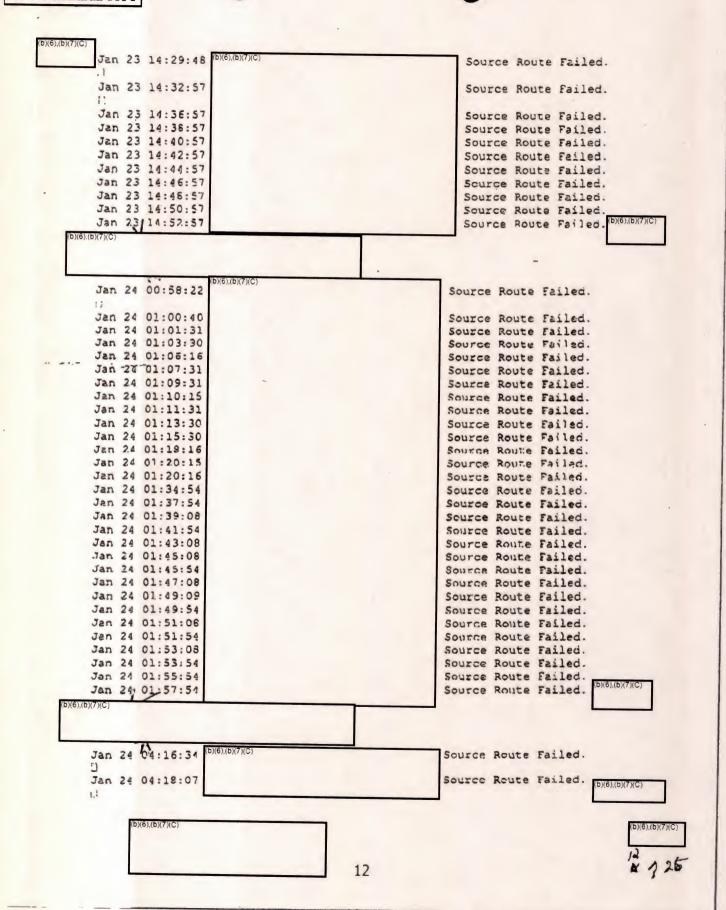
. . . . . . . .

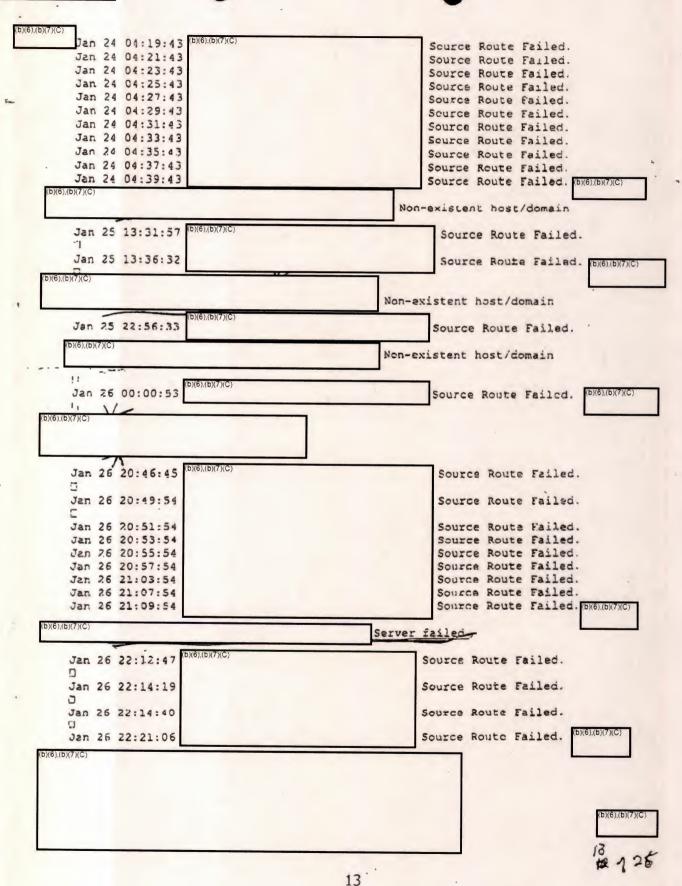












	Source Route Failed. (b)(6),(b)(7)(C) Source Route Failed.
(b)(6),(b)(7)(C)	
Jan 27 05:26:57 (b)(6),(b)(7)(C) Jan 27 05:26:59	Source Route Failed.
(b)(6),(b)(7)(C)	Source Route Failed. (b)(6),(b)(7)(C)
	Non-existent host/domain
Jan 27 05:48:20 (b)(6),(b)(7)(C)	Source Route Failed.
Jan 27 05:48:32	Source Route Failed. (b)(6)(b)(7)(C)
Jan 27 05:49:59 (b)(6),(b)(7)(C)	Source Route Failed.
Phys) (hy7yC)	
Jan 28 21:35:42 (b)(6),(b)(7)(C)	protocol unreachable (b)(
Jan 31 03:20:50 (b)(6),(b)(7)(C)	Source Route Failed.
11	Source Noute latted.
(b)(6),(b)(7)(C)	
	Non-existent host/domain
Feb 1 14:26:39 (b)(6),(b)(7)(C)	Source Route Failed.
Feb 1 14:26:39 (D)(6),(D)(7)(C) Feb 1 14:26:42	Source Route Failed. Source Route Failed.
Feb 1 14:26:39 (b)(6),(b)(7)(C) Feb 1 14:26:42 Feb 1 14:28:12	Source Route Failed. Source Route Failed. Source Route Failed.
Feb 1 14:26:39 (D)(6),(D)(7)(C) Feb 1 14:26:42	Source Route Failed. Source Route Failed.
Feb 1 14:26:39 (b)(6)(b)(7)(C) Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48	Source Route Failed.
Feb 1 14:26:39 (b)(6)(b)(7)(C) Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:40	Source Route Failed.
Feb 1 14:26:39 (b)(6)(b)(7)(C) Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:46 Feb 1 14:37:46	Source Route Failed.
Feb 1 14:26:39 (b)(6)(b)(7)(C) Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:46 Feb 1 14:37:46 Feb 1 14:39:48	Source Route Failed.
Feb 1 14:26:39 (b)(6)(b)(7)(C) Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:46 Feb 1 14:37:46	Source Route Failed.
Feb 1 14:26:39 Feb 1 14:26:42 Feb 1 14:26:42 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:40 Feb 1 14:37:46 Feb 1 14:39:48 Feb 1 14:41:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:45:48	Source Route Failed.
Feb 1 14:26:39 Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:40 Feb 1 14:37:46 Feb 1 14:39:48 Feb 1 14:41:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:47:48	Source Route Failed.
Feb 1 14:26:39 Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:40 Feb 1 14:37:46 Feb 1 14:39:48 Feb 1 14:41:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:47:48 Feb 1 14:47:48 Feb 1 14:47:48 Feb 1 14:47:48	Source Route Failed.
Feb 1 14:26:39 Feb 1 14:26:42 Feb 1 14:28:12 Feb 1 14:29:46 Feb 1 14:31:46 Feb 1 14:33:48 Feb 1 14:35:40 Feb 1 14:37:46 Feb 1 14:39:48 Feb 1 14:41:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:43:48 Feb 1 14:47:48	Source Route Failed.

